

WHAT IS CLAIMED IS:

- 1 1. A method for enabling access to data in a storage medium within one
2 of a plurality of storage cartridges capable of being mounted into a interface device,
3 comprising:
4 providing an association of at least one coding key to a plurality of storage
5 cartridges;
6 determining one coding key associated with one target storage cartridge,
7 wherein the coding key is capable of being used to access data in the storage medium
8 within the target storage cartridge; and
9 encrypting the determined coding key, wherein the coding key is decrypted to
10 use to decode and code data stored in the storage medium.
- 1 2. The method of claim 1, further comprising:
2 using the coding key to encode data to write to the storage medium;
3 transmitting the encoded data to the interface device to write to the storage
4 medium in one storage cartridge mounted in the interface device;
5 receiving encoded data from the interface device read from the storage
6 medium; and
7 using the coding key to decrypt the received encoded data.
- 1 3. The method of claim 1, wherein the association of the at least one
2 coding key to the plurality of storage cartridges associates one key with the plurality
3 of storage cartridges, wherein the one key is capable of being used to encode data
4 written to the storage medium and decode data read from the storage medium of the
5 plurality of storage devices.
- 1 4. The method of claim 1, wherein the association of the at least one
2 coding key to the plurality of storage cartridges associates a different key with each
3 storage cartridge, wherein the key associated with one storage cartridge is used to

4 encode data written to the storage medium and decode data read from the storage
5 medium of the storage cartridge.

1 5. The method of claim 1, wherein the coding key comprises a seed value
2 that is used to generate an additional key that is used to directly decode and encode
3 the data in the storage medium in the storage cartridge.

1 6. The method of claim 1, further comprising:
2 transmitting the encrypted coding key to the interface device, wherein the
3 interface device decrypts the coding key to use to decode and code data stored in the
4 storage medium.

1 7. The method of claim 6, wherein encrypting the coding key further
2 comprises:
3 encrypting the coding key with a first key, wherein a second key used by the
 interface device is capable of decrypting the coding key encrypted with the first key.

1 8. The method of claim 6, wherein encrypting the coding key further
2 comprises:
3 encrypting the coding key with a first key, wherein a second key is capable of
4 decrypting the coding key encrypted with the first key;
5 encrypting the second key with a third key, wherein a fourth key used by the
6 interface device is capable of decrypting data encrypted with the third key; and
7 transmitting the coding key encrypted with the first key and the second key
8 encrypted with the third key to the interface device.

1 9. The method of claim 6, wherein encrypting the coding key further
2 comprises:
3 encrypting the coding key with a first key, wherein a second key is capable of
4 decrypting the coding key encrypted with the first key;
5 transmitting the coding key encrypted with the first key to the interface
6 device;
7 receiving, from the interface device, the coding key encrypted with the first
8 key;
9 decrypting the coding key with the second key;
10 encrypting the coding key with a third key, wherein a fourth key used by the
11 interface device is capable of decrypting data encrypted with the third key; and
12 transmitting the coding key encrypted with the third key to the interface
13 device.

1 10. A method for accessing data in a removable storage cartridge
2 including a storage medium, comprising:
3 receiving an encrypted coding key from a host system;
4 decrypting the encrypted coding key;
5 using the coding key to encode data to write to the storage medium; and
6 using the coding key to decode data written to the storage medium.

1 11. The method of claim 10, wherein encoding the data with the coding
2 key compresses the data and wherein decoding the data written to the storage medium
3 decompresses the data, and wherein the data can only be encoded or decoded using
4 the coding key.

1 12. The method of claim 10, wherein the coding key is encrypted by a first
2 key maintained at the host system, further comprising:
3 maintaining a second key that is capable of decrypting data encrypted using
4 the first key, wherein the second key is used to decrypt the coding key encrypted with
5 the first key.

1 13. The method of claim 12, wherein the second key is stored in an
2 integrated circuit non-volatile memory that is only accessible to decrypting logic that
3 uses the second key to decrypt data encrypted using the first key.

1 14. The method of claim 13, further comprising:
2 transmitting the coding key decrypted using the decrypting logic to
3 encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to
4 encode and decode data to the storage medium.

1 15. The method of claim 12, further comprising:
2 storing the coding key encrypted with the first key within the storage
3 cartridge;
4 receiving an input/output (I/O) request directed to the storage cartridge; and
5 accessing the encrypted coding key from the storage cartridge, wherein the
6 accessed coding key is decrypted using the second key, and wherein the decrypted
7 coding key is used to encode and decode data to execute the I/O request to the storage
8 cartridge.

1 16. The method of claim 10, wherein the received encrypted coding key is
2 encrypted by a first key maintained at the host system, wherein the host system
3 maintains a second key that is capable of decrypting data encrypted using the first
4 key, further comprising:

5 receiving, from the host system, the second key encrypted by the host system
6 using a third key, wherein data encrypted using the third key is capable of being
7 decrypted using a fourth key;
8 accessing the fourth key;
9 using the fourth key to decrypt the encrypted second key received from the
10 host system; and
11 using the decrypted second key to decrypt the received coding key encrypted
12 using the first key.

1 17. The method of claim 10, wherein the coding key is encrypted by a first
2 key maintained at the host system, wherein the host system maintains a second key
3 that is capable of decrypting data encrypted using the first key, further comprising:
4 transmitting the encrypted coding key received from the host system back to
5 the host system; and
6 in response to transmitting the encrypted coding key back to the host system,
7 receiving, from the host system, the coding key encrypted using a third key, wherein
8 data encrypted using the third key is decrypted using a fourth key; and
9 accessing the fourth key, wherein the coding key is decrypted using the fourth
10 key.

1 18. A system for enabling access to data in a storage medium within one
2 of a plurality of storage cartridges, comprising:
3 an interface device in which the storage cartridges are capable of being
4 mounted, wherein the interface device is capable of writing data to the storage
5 medium within the storage cartridges and reading data from the storage medium in
6 the storage cartridges;
7 means for determining one coding key associated with one target storage
8 cartridge, wherein the coding key is capable of being used to access data in the
9 storage medium within the target storage cartridge; and

10 means for encrypting the determined coding key, wherein the coding key is
11 decrypted to use to decode and encode data stored in the storage medium.

1 19. The system of claim 18, further comprising:
2 means for using the coding key to encode data to write to the storage medium;
3 means for transmitting the encoded data to the interface device to write to the
4 storage medium in one storage cartridge mounted in the interface device;
5 means for receiving encoded data from the interface device read from the
6 storage medium; and
7 means for using the coding key to decrypt the received encoded data.

1 20. The system of claim 18, wherein the association of the at least one
2 coding key to the plurality of storage cartridges associates one key with the plurality
3 of storage cartridges, wherein the one key is capable of being used to encode data
4 written to the storage medium and decode data read from the storage medium of the
5 plurality of storage devices.

1 21. The system of claim 18, wherein the association of the at least one
2 coding key to the plurality of storage cartridges associates a different key with each
3 storage cartridge, wherein the key associated with one storage cartridge is used to
4 encode data written to the storage medium and decode data read from the storage
5 medium of the storage cartridge.

1 22. The system of claim 18, further comprising:
2 means for transmitting the encrypted coding key to the interface device,
3 wherein the interface device decrypts the coding key to use to decode and code data
4 stored in the storage medium.

1 23. A system for accessing data in a removable storage cartridge including
2 a storage medium, comprising:
3 means for receiving an encrypted coding key from a host system;
4 means for decrypting the encrypted coding key;
5 means for using the coding key to encode data to write to the storage medium;
6 and
7 means for using the coding key to decode data written to the storage medium.

1 24. The system of claim 23, wherein the coding key is encrypted by a first
2 key maintained at the host system, further comprising;
3 means for maintaining a second key that is capable of decrypting data
4 encrypted using the first key, wherein the second key is used to decrypt the coding
5 key encrypted with the first key.

1 25. The system of claim 24, further comprising:
2 an integrated circuit non-volatile memory including the second key, wherein
3 the integrated circuit non-volatile memory;
4 decrypting logic for using the second key to decrypt data encrypted using the
5 first key, wherein the integrated circuit non-volatile memory is only accessible to the
6 decrypting logic.

1 26. The method of claim 24, further comprising:
2 means for storing the coding key encrypted with the first key within the
3 storage cartridge;
4 means for receiving an input/output (I/O) request directed to the storage
5 cartridge; and
6 means for accessing the encrypted coding key from the storage cartridge,
7 wherein the accessed coding key is decrypted using the second key, and wherein the

8 decrypted coding key is used to encode and decode data to execute the I/O request to
9 the storage cartridge.

1 27. An article of manufacture including code for enabling access to data in
2 a storage medium within one of a plurality of storage cartridges capable of being
3 mounted into a interface device, wherein the code is capable of causing operations
4 comprising:

5 providing an association of at least one coding key to a plurality of storage
6 cartridges;

7 determining one coding key associated with one target storage cartridge,
8 wherein the coding key is capable of being used to access data in the storage medium
9 within the target storage cartridge; and

10 encrypting the determined coding key, wherein the coding key is decrypted to
11 use to decode and code data stored in the storage medium.

1 28. The article of manufacture of claim 27, further comprising:

2 using the coding key to encode data to write to the storage medium;

3 transmitting the encoded data to the interface device to write to the storage
4 medium in one storage cartridge mounted in the interface device;

5 receiving encoded data from the interface device read from the storage
6 medium; and

7 using the coding key to decrypt the received encoded data.

1 29. The article of manufacture of claim 27, wherein the association of the
2 at least one coding key to the plurality of storage cartridges associates one key with
3 the plurality of storage cartridges, wherein the one key is capable of being used to
4 encode data written to the storage medium and decode data read from the storage
5 medium of the plurality of storage devices.

1 30. The article of manufacture of claim 27, wherein the association of the
2 at least one coding key to the plurality of storage cartridges associates a different key
3 with each storage cartridge, wherein the key associated with one storage cartridge is
4 used to encode data written to the storage medium and decode data read from the
5 storage medium of the storage cartridge.

1 31. The article of manufacture of claim 27, wherein the coding key
2 comprises a seed value that is used to generate an additional key that is used to
3 directly decode and encode the data in the storage medium in the storage cartridge.

1 32. The article of manufacture of claim 27, further comprising:
2 transmitting the encrypted coding key to the interface device, wherein the
3 interface device decrypts the coding key to use to decode and code data stored in the
4 storage medium.

1 33. The article of manufacture of claim 32, wherein encrypting the coding
2 key further comprises:
3 encrypting the coding key with a first key, wherein a second key used by the
 interface device is capable of decrypting the coding key encrypted with the first key.

1 34. The article of manufacture of claim 32, wherein encrypting the coding
2 key further comprises:
3 encrypting the coding key with a first key, wherein a second key is capable of
4 decrypting the coding key encrypted with the first key;
5 encrypting the second key with a third key, wherein a fourth key used by the
6 interface device is capable of decrypting data encrypted with the third key; and
7 transmitting the coding key encrypted with the first key and the second key
8 encrypted with the third key to the interface device.

U.S. PATENT & TRADEMARK OFFICE

1 35. The article of manufacture of claim 32, wherein encrypting the coding
2 key further comprises:
3 encrypting the coding key with a first key, wherein a second key is capable of
4 decrypting the coding key encrypted with the first key;
5 transmitting the coding key encrypted with the first key to the interface
6 device;
7 receiving, from the interface device, the coding key encrypted with the first
8 key;
9 decrypting the coding key with the second key;
10 encrypting the coding key with a third key, wherein a fourth key used by the
11 interface device is capable of decrypting data encrypted with the third key; and
12 transmitting the coding key encrypted with the third key to the interface
13 device.

1 36. An article of manufacture including code for accessing data in a
2 removable storage cartridge including a storage medium, wherein the code causes
3 operations comprising:
4 receiving an encrypted coding key from a host system;
5 decrypting the encrypted coding key;
6 using the coding key to encode data to write to the storage medium; and
7 using the coding key to decode data written to the storage medium.

1 37. The article of manufacture of claim 36, wherein encoding the data
2 with the coding key compresses the data and wherein decoding the data written to the
3 storage medium decompresses the data, and wherein the data can only be encoded or
4 decoded using the coding key.

1 38. The article of manufacture of claim 36, wherein the coding key is
2 encrypted by a first key maintained at the host system, further comprising:
3 maintaining a second key that is capable of decrypting data encrypted using
4 the first key, wherein the second key is used to decrypt the coding key encrypted with
5 the first key.

1 39. The article of manufacture of claim 38, wherein the second key is
2 stored in an integrated circuit non-volatile memory that is only accessible to
3 decrypting logic that uses the second key to decrypt data encrypted using the first
4 key.

1 40. The article of manufacture of claim 36, further comprising:
2 transmitting the coding key decrypted using the decrypting logic to
3 encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to
4 encode and decode data to the storage medium.

1 41. The article of manufacture of claim 38, further comprising:
2 storing the coding key encrypted with the first key within the storage
3 cartridge;
4 receiving an input/output (I/O) request directed to the storage cartridge; and
5 accessing the encrypted coding key from the storage cartridge, wherein the
6 accessed coding key is decrypted using the second key, and wherein the decrypted
7 coding key is used to encode and decode data to execute the I/O request to the storage
8 cartridge.

1 42. The article of manufacture of claim 36, wherein the received encrypted
2 coding key is encrypted by a first key maintained at the host system, wherein the host
3 system maintains a second key that is capable of decrypting data encrypted using the
4 first key, further comprising:

5 receiving, from the host system, the second key encrypted by the host system
6 using a third key, wherein data encrypted using the third key is capable of being
7 decrypted using a fourth key;
8 accessing the fourth key;
9 using the fourth key to decrypt the encrypted second key received from the
10 host system; and
11 using the decrypted second key to decrypt the received coding key encrypted
12 using the first key.

1 43. The article of manufacture of claim 36, wherein the coding key is
2 encrypted by a first key maintained at the host system, wherein the host system
3 maintains a second key that is capable of decrypting data encrypted using the first
4 key, further comprising:
5 transmitting the encrypted coding key received from the host system back to
6 the host system; and
7 in response to transmitting the encrypted coding key back to the host system,
8 receiving, from the host system, the coding key encrypted using a third key, wherein
9 data encrypted using the third key is decrypted using a fourth key; and
10 accessing the fourth key, wherein the coding key is decrypted using the fourth
11 key.